Information Commissioner
NORTHERN TERRITORY

Annual Report

2023/24

Access to Information | Privacy Protection

Acknowledgement of Country

Our Office acknowledges the traditional owners of the Northern Territory and recognises their continuing cultural and spiritual connections to their lands, waters and communities. We pay our respects to all Aboriginal and Torres Strait Islander people and their cultures, their elders past and present, and to future generations.

Table of Contents

Message from the Commissioner

This is my last report as NT Information Commissioner. I commenced in the role in March 2003 as the inaugural Commissioner and served until mid-2007, thereafter holding a number of other positions until I took the role on again from August 2018. Prior to my initial appointment, I had worked with the Queensland Information Commissioner for nine years.

It has been a privilege to hold this, and various other appointments, in the service of the NT community. In doing so, I have always strived to promote good government, enhancing transparency and accountability, while recognising the importance of protecting individual rights and private interests.

As always, government faces many challenges and must deal with them in the context of limited resources and myriad competing expectations and demands. Even so, decades of experience in these areas have done nothing but strengthened my conviction that enhancing government transparency and accountability and privacy protection are key expectations of the community and demand due attention and priority from government.

In the busy daily lives of community members, accountability and privacy are not necessarily 'front of mind' issues. Their power lies in underpinning the essence of good government. Their consequence comes to the fore when there is a substantial breach of community expectations. That is when their fundamental significance to the community becomes very clear. It is when a breach of integrity or a major breach of privacy surfaces, that the slumbering giant of public opinion stirs and can move mountains and governments.

This potential (and the need to address it before it manifests) lies at the heart of accountability measures like FOI, privacy protection and the various independent oversight bodies. They are designed to bring accountability to the fore, to act as constant mechanisms to remind and encourage all arms of government to do the right thing by the community and the individuals they serve.

In order to maintain integrity and public trust, it is vital for government to maintain the effectiveness of these mechanisms by ensuring they are given the support, priority and resources they require.

With that in mind, I raise below a number of broader issues for consideration by the NT Government.

The need for contemporary legislation to meet current and future risks and demands where privacy and data security are concerned has never been more apparent. The *Information Act 2002* (the **Act**), which regulates the FOI scheme and privacy protection within public sector organisations (**Organisations**), is over 20 years old and overdue for review. Although successive governments have made limited amendments over time, no holistic review has ever been completed and actioned.

Identifying what reforms are required to the areas of FOI, privacy law and records management is no easy task and requires expert advice to ensure that any changes are workable and effective at protecting the public interest in years to come. It is hoped that work on appropriate reform will occur and proceed to a concrete conclusion within the foreseeable future.

On another point, it is essential that a sufficient level of resourcing is provided to support an FOI scheme that is patently under considerable strain. There is no doubt that the public still supports the scheme as is shown by the ever-increasing numbers of applications made. The level of access applications is 2½ times what it was when the scheme first started and has increased by 70% in the last five years. In the face of such increases, the capacity of Organisations and my Office to effectively administer and oversight the scheme is at risk.

In 2022, a centralised FOI Unit for NT Government agencies was established to assist with the administration of FOI applications across government. Some agencies utilised the FOI Unit from the outset while others have joined the centralised Unit at later times.[1] All agencies using the centralised model remain responsible for identifying the documents sought and they must ultimately make the decisions on what documents are released through the FOI scheme.

From our observations and informal feedback from stakeholders, this has brought measurable benefits for Organisations that historically manage small numbers of applications per year. However, the benefits remain uncertain for agencies that have traditionally maintained dedicated teams managing high volumes of applications.

At the time of its formation, I commented that a centralised unit should not be created in the hope of reducing the cost of FOI administration across government. The new system necessarily requires a double handling of information at many stages in the process but its ability to build and retain an experienced team should ensure a more consistent and informed approach to FOI administration.

However, a centralised model will only assist service delivery into the future if it is sufficiently resourced to attract and maintain experienced staff. After over 2 years of operation, a review of the FOI Unit, including its resource requirements, should be considered. Agency staff must also be properly trained in tasks such as identifying the information sought, assisting with clarification of the reasonable scope of an application and making sound and lawful decisions.

In this world of big data, hyperconnectivity and AI, there is an ever-increasing need for Organisations (both local and NT government) to be able to seek advice from privacy experts when designing new initiatives and technologies. I give examples in my report of considerable advice my Office has provided to Organisations on privacy, information sharing and data security, often to the detriment of other work that my Office is required to undertake. Good advice is imperative to ensure that data security risks are minimised and the public's trust in government is maintained.

[1] In July 2023, FOI applications for Correctional Services and WorkSafe NT were included in the centralised management model and in December 2023, the Department of Health moved all administrative responsibilities for its FOI applications to the centralised Unit. NT Police has also recently moved to the centralised model.

For my Office, after two decades of minimal change to our budget, it is time to consider an independent review of our resources to ensure that we are able to continue to provide professional/expert advice on privacy and FOI, as well as conduct our other functions, in a timely manner. The NT Government and Organisations themselves must also recognise the need for sufficient resources to dedicate to their own internal management to ensure they encourage and retain strong data management and information sharing systems, good governance, policy development and training to protect the public interest where privacy is concerned.

Data breach management is one area that I consider deserves immediate attention. Data breaches happen – it is all about minimising risk and protecting individuals and the Territory from harm. I acknowledge that work is being done to provide a cross-government data breach management framework, but I encourage a more prioritised response to this important body of work. For example, cross-government education, training and guidance on data breach management should occur as a priority. I also maintain my call for a legislative data breach notification scheme requiring serious data breaches to be reported to my Office and to victims of breaches.

Two specific bodies of work undertaken during this reporting period deserve special mention.

Over the past two years, my Office has been involved in providing advice on a new legislatively sanctioned information sharing scheme to assist Territory Families in keeping at-risk children safe. The steps taken by the lead agencies to design and build a model that facilitates information sharing about families within acceptable limits are to be commended. In particular, I note the considerable legal advice obtained, the independent privacy impact assessments undertaken, and Grants of Authorisation sought and obtained throughout the development stage. It is important that equivalent care is taken with every new information sharing initiative to ensure that the outcome maintains the right balance between the public interest generally and the reasonable protection of individual privacy.

Secondly, a Domestic Violence Information Sharing Report, *A Matter of Trust*, was tabled in March 2024 reviewing the operation of the Chapter 5A information sharing scheme under the *Domestic and Family Violence Act 2007*. It is still early days in a scheme that was introduced to assist stakeholder organisations and agencies to share information to keep women and their children safe. Often with legislative changes to support information sharing, it does take time for a new process to be accepted, particularly if the information being shared is sensitive and personal to a vulnerable group. It is unclear and perhaps doubtful whether the Chapter 5A scheme has been sufficiently utilised by enough stakeholders to be considered a success. If government wants the scheme to reach its full potential, there will need to be more consultation, education, training and support provided to stakeholder organisations. A 5 year review by my Office is due to commence in 2025 but is currently unfunded. It is essential that the lead agency provide appropriate support to our small Office to enable us to undertake the 5 year review in a comprehensive and timely manner.

Finally, I thank the staff of the Office, and particularly Deputy Commissioner (and former Commissioner) Brenda Monaghan, for their tireless efforts in promoting the objects of the Office, which I regard as essential to maintaining integrity and protecting essential human rights in government.

Peter Shoyer
Information Commissioner
26 September 2024

Introduction

The *Information Act 2002* (the **Act**) is the legislation governing freedom of information (**FOI**), privacy protection, and public sector records management in the NT. The Act provides for reasonable public access to government information, the responsible collection, correction and handling of personal information and appropriate records and archives management.

The Act is intended to strike a balance between competing interests of openness and transparency and the legitimate protection of some government information, including personal information about individuals.

The Act establishes an Information Commissioner to oversight information access and privacy protection provisions. The Information Commissioner's functions include:

- dealing with complaints about FOI decisions and privacy issues through an investigation and mediation process;
- referring, at the request of a party, dismissed or unresolved complaints to the NT Civil and Administrative Tribunal (**NTCAT**) for hearing;
- commenting on the privacy implications of new legislation and government initiatives;
- conducting privacy audits of records held by public sector organisations;
- considering applications for grants of authorisation made by public sector organisations to collect, use or disclose personal information in a manner that would otherwise contravene the Information Privacy Principles;
- considering applications for extension of time periods relating to certain exemptions, e.g. the business information exemption (section 57 of the Act); and
- educating the public and public officers about FOI and privacy protection.

Since August 2018 the Office of the Information Commissioner (**OIC**) has been located within the Ombudsman's Office. Despite its location and utilisation of shared corporate support, the OIC remains an independent statutory office with a memorandum of understanding between itself and the Ombudsman's Office that covers information sharing and referrals between the offices.

The resources of the OIC are very limited. The Commissioner and Deputy have dual roles (i.e. they are also Ombudsman and Deputy Ombudsman respectively) and so are able to contribute only part of their time to OIC functions. Apart from this, the OIC is currently comprised of two full-time positions - a Senior Policy and Investigation Officer and an Administrative Policy and Complaints Officer. Necessary corporate support is provided by the Business Services Unit of the Ombudsman's Office.

During this reporting period, an additional short-term position was provided by Territory Families to assist the Commissioner in advising on privacy issues arising from the 360VOC data sharing project.

Freedom of Information

Annual statistics

New FOI applications received by all public sector organisations for the financial year 2023/24. An increase of 8% compared with 2022/23.

FOI applications finalised by public sector organisations for the financial year 2023/24. An increase of 7% compared to 2022/23.

of new applications were for personal information about the applicant only.

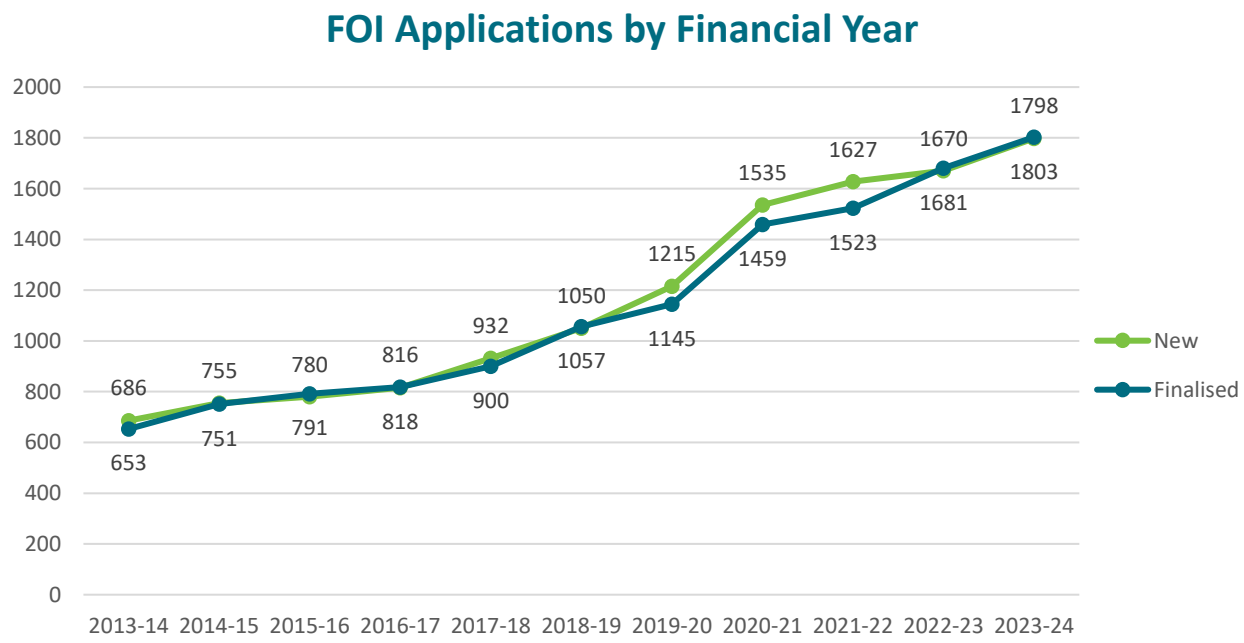
of new applications were for non-personal information only.

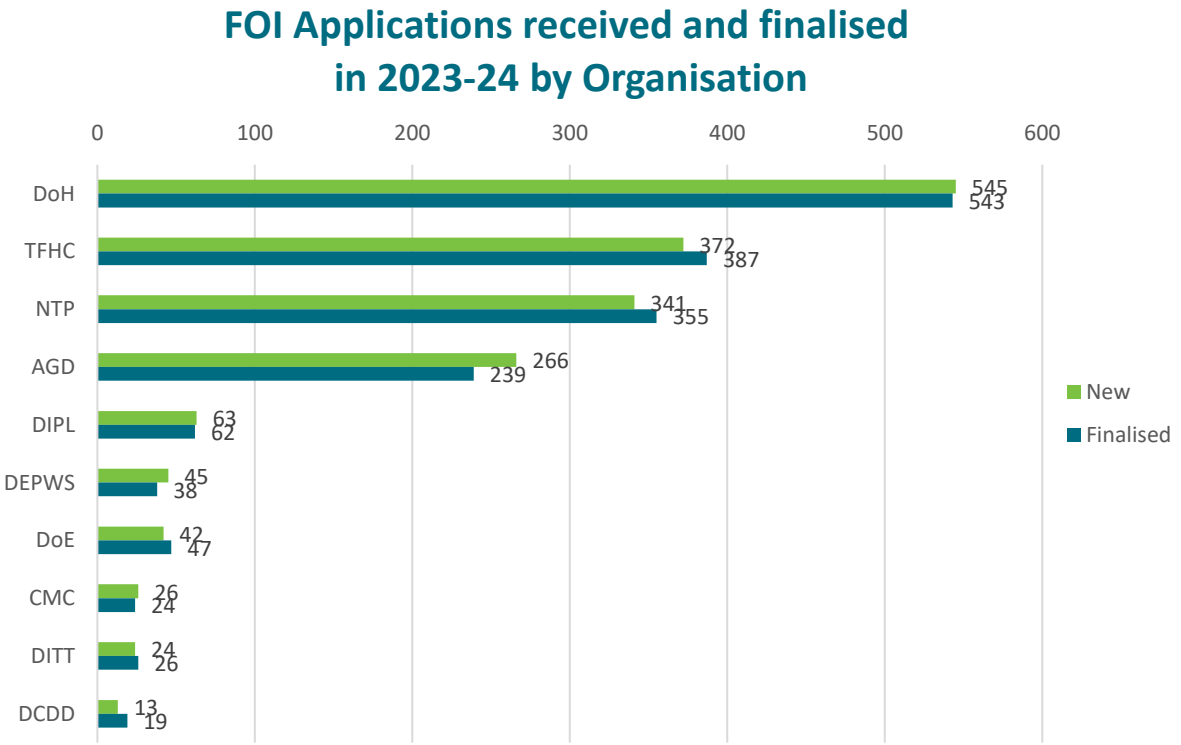
of new applications were from political, media, activist or lobby groups.

FOI applications

Trends

FOI applications received by public sector organisations (**Organisations**) continued to trend upward in 2023/24. The total number of FOI applications submitted to Organisations has increased by 7% in the past year and over 70% in the past 5 years. Despite the rising demand for access to government information, Organisations appear to have seen little change in resource allocation to respond to the increased numbers.





Note: See Appendix 2 for the full names of abbreviated public sector organisations referred to in the graph.

In the past 5 years, the Department of Health (**DoH**) has experienced an increase of over 50%[2] in applications received, with 82% of applications in 2023/24 being requests for personal information. This year, DoH received more applications by far than any other Organisation, experiencing an increase of over 20% compared to 2022/23.

Comment from FOI officers dealing with these applications is that the significant rise in applications submitted to DoH can largely be attributed to a strong interest by members of the public in accessing their own health information.

The Department of Attorney-General and Justice (**AGD** - which included Correctional Services) experienced an increase of 37% in applications over the previous year, with 76% of applications being requests for personal information. NT Police (**NTP**) recorded an increase of 14% compared with 2022/23.

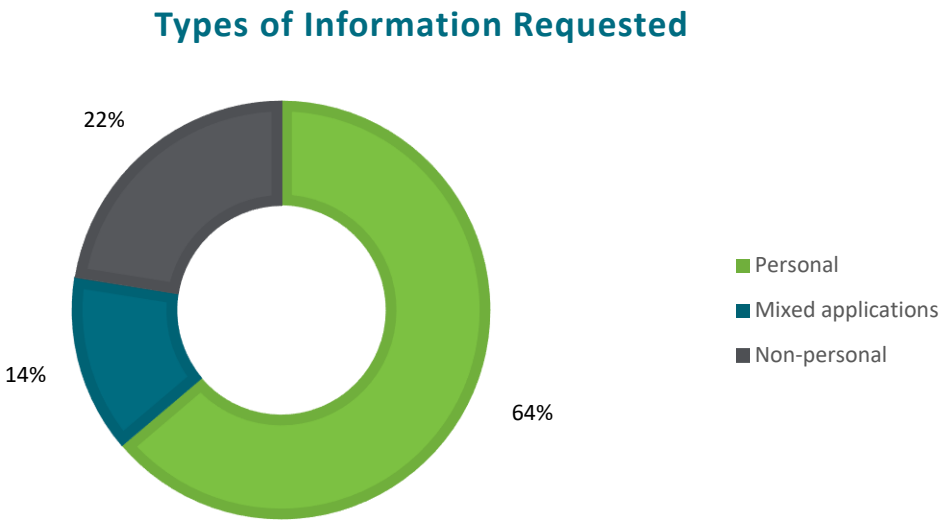
On the other hand, Territory Families, Housing and Communities (**TFHC**) applications fell by 16%.

Types of information requested

Most FOI applications submitted to Organisations in 2023/24 were for personal information (64%), being applicants seeking information about themselves. Examples of personal information sought could be an individual's health record held with DoH or information held about them on a TFHC file.

A further 22% of applications were for non-personal information, being other government information held by an Organisation and 14% were for a combination of both personal and non-personal information.

Of all applications made, 8% were from individuals with a political, media, activist, or lobby-group background.



[2] 348 in 2018/19.

The FOI process and outcomes

There is a growing understanding within the general public of their right to seek access to recorded information held by Organisations. Transparency and government accountability are the touchstones of the FOI process.

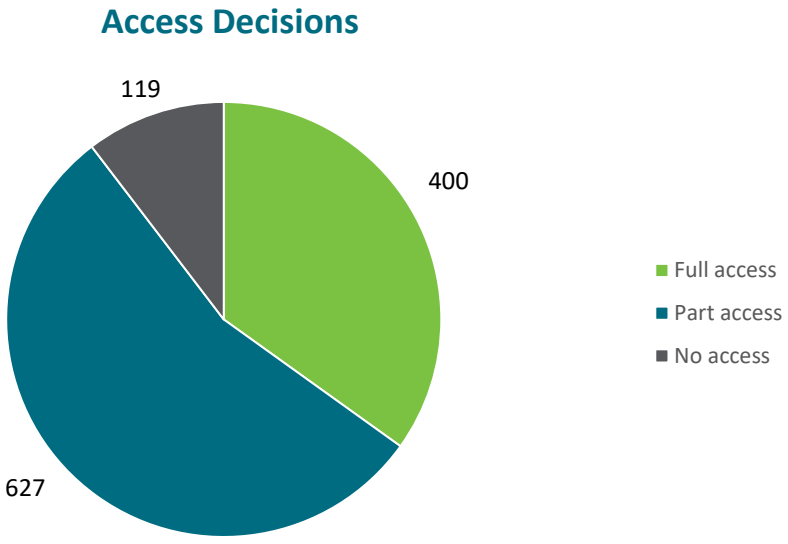
While an applicant does not need to provide their reason for requesting information, they must meet certain legislative requirements for a valid application. Organisations should always make their best efforts to assist an applicant to make or vary their application so that it meets those requirements but even so, a significant number of applications are refused due to such issues. There are also cases where the records sought do not exist or cannot be found or do not fall within the scope of the Act.

Most applications do not face such issues. In the majority of cases, Organisations decide either to release the records sought in full or to refuse access to some or all of the information sought on the basis of one or more of the exemptions in Part 4 of the Act, *Exemptions in the public interest*. We call this an '**access decision'**.

We will first discuss outcomes of access decisions before moving on to applications finalised because there has been an unresolved technical or procedural issue with their application.

Access granted

A primary object of the Act is to provide a general right of access to government held information and a request under the Act is a separate process to the administrative access schemes that many Organisations also have in place. The Act does not stop Organisations from releasing information proactively and the FOI scheme is often relied on by Organisations when a request from an individual is complex, extensive or has specific sensitivities.



In 2023/24, 35% of access decisions resulted in the requested information being released to the applicant in full, which is slightly higher than the 2022/23 figures of 32%.

Access refused under exemption

A further 55% of access decisions resulted in disclosure of part of the information requested, which is slightly lower than the 2022/23 figure of 61%. This means 90% of access decisions resulted in the applicant getting access to all or some of the information sought.

The other 10% of access decisions resulted in no records being provided to the applicant. This was an increase from 7% in 2022/23. However, comparison with most recent figures from other Australian jurisdictions[3] for 2022/23 would still have placed the NT at 10% in the mid-range in this regard (with four jurisdictions lower and four jurisdictions higher).

Even so, the increase is of some note compared to 3% or 4% in a number of recent years. Two thirds of the applications refused in full involved NT Police, which advises that the bulk of those applications (84%) were refused on the basis of the *Preservation of system of justice*, *Security and law enforcement* or *Ombudsman Act* exemption.

A significant number of these applications were refused under section 49(c) of the Act, which exempts information if disclosure would disclose information about a proceeding or other matter before a court or tribunal. In my view, section 49(c) does not operate as a blanket exemption and should be read and applied narrowly.[4]

During the period, the most widely used exemptions were those aimed at protecting:

- the privacy of individuals (section 56) – relied upon by 16 Organisations;
- deliberative processes (section 52) and confidentially obtained information (section 55) – relied upon by 9 Organisations;
- the system of justice (section 49) – relied upon by 8 Organisations; and
- commercial and business information (section 57) – relied upon by 7 Organisations.

Making and progressing a valid application

An access application must meet the requirements of section 18 of the Act to be valid. It must be in writing, specify the name and contact address of the applicant and include sufficient details to identify the information sought. It must also be accompanied by the application fee (unless waived by the Organisation). Finally, before accepting the application, an Organisation must satisfy itself as to the identity of the applicant.

A valid application may be withdrawn by the applicant or transferred to another Organisation.

---

[3] Figures for 2022/23 can be found at: https://www.ipc.nsw.gov.au/information-access/open-government-open-data/dashboard .

[4] The Information Commissioner's Guideline: A Guide to FOI Exemptions (published in August 2017) at p25 notes:
"… section 49 is aimed at ensuring that freedom of information does not infringe judicial and quasi-judicial practices and procedures. This suggests the exemption will only apply:
- *to a matter currently before a court or tribunal at the time a decision is being made;*
- *in a narrow sense to documents 'about' a proceeding or other matter, meaning that the documents must not simply relate to the same topic as that which is also a proceeding, but must actually disclose something about the court or tribunal proceeding (e.g. a Memo to a CEO providing an update on proceedings would be 'about' the proceedings) …"*

An Organisation may also decide not to progress an application for other reasons, including:

- the information is already publicly available;
- a required deposit or processing fee has not been paid;
- the information sought cannot be identified or found or does not exist;
- the information is excluded from, or does not come within, the Act; or
- providing access would unreasonably interfere with its operations.

There is a clear expectation that, as far as possible, Organisations will communicate with an applicant in a genuine effort to rectify any problems or deficiencies with an application in a manner that will enable the application to progress effectively. This may involve several rounds of discussion to clarify or refine its scope.

Even so, a large number of applications are finalised on these other grounds. Most prevalent among those during 2023/24 were approaches that did not meet the requirements for a valid application under section 18 (211), followed by cases where the information sought could not be identified or found or did not exist (201).

A breakdown of those other outcomes by Organisation is set out at Appendix 2, Table 1A.

During 2023/24, the large number of refusals by DoH under section 18 primarily consisted of applications by insurance agencies seeking to access government information and then failing to pay application fees. DoH anticipates a drop in the number of such refusals however, as insurance-related applications are again being processed by the Organisation through an administrative scheme rather than through an FOI application.

Many applications to DoH were also refused under section 18 in circumstances where ID was not provided by representatives of applicants (such as legal firms). Once again, the number of such refusals should decrease in 2024/25 following consultation between the FOI team and representatives of applicants regarding ID requirements.

A large number of refusals were made by TFHC on the basis that the information sought cannot be identified or found or does not exist. It is understood that TFHC receives a significant volume of requests for historical information, including requests relating to the National Redress Scheme. These applicants often seek historical information about themselves or their family in broad terms covering significant periods of time. Applications of this nature rely heavily on the recall of applicants and can have little to no detail to assist TFHC in identifying the information sought. If records are unable to be identified based on the provided terms, they will usually be referred to the National Archives which may hold the records under request.

Review processes

If an applicant is not satisfied with the initial access decision they receive from an Organisation, they can ask for an internal review by an independent officer to allow the Organisation the opportunity to reconsider its initial decision. If an applicant is still not satisfied after an internal review, they have a right of complaint to the OIC. There is also a provision for an Organisation to refer an application for internal review directly to the OIC as a complaint (section 39A referrals).

The percentage of initial applications that progressed to internal review rose significantly from 2% in 2022/23 to 5% in 2023/24. The majority of those 82 applications were to Police (30, up from 12) and AGD (20, up from 5). No specific reason for the increases in relation to those two Organisations has been identified.

Of the internal reviews where a decision was made by the Organisation during 2023/24, 60% confirmed the initial decision and 40% revoked or varied the initial decision.

In 2023/24, 11% of internal review applications were transferred directly to the OIC under section 39A of the Act. Historically, Organisations choose this path of referral when they are confident that the initial decision is accurate and there are no further submissions to consider or where the Organisation does not have the resources to undertake an internal review process. However, most Organisations prefer to take advantage of the opportunity to reconsider their initial decision.

FOI Matters by Stage

	2022/23	2023/24
Total FOI applications received by Organisations	1,670	1,798
Internal review applications	40	82
Referred to OIC without internal review	0	9
Complaints to OIC after internal review	15	20

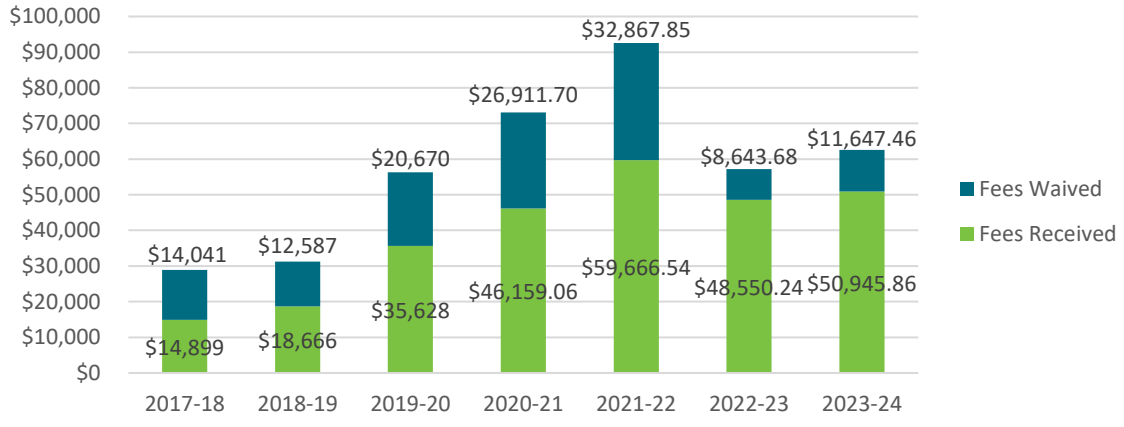
Application and processing fees

The Act provides for charging of application fees and processing fees. Similar to other jurisdictions, the maximum fees chargeable are set in legislation at a level well below that required for Organisations to recover the costs of administering the FOI scheme.

The fees are intended to act as a reasonable check on multiple and unnecessarily widely scoped applications as they require an applicant to demonstrate their commitment to obtaining the information by assisting with associated costs.

No application fees are chargeable for requests for purely personal information and most Organisations rarely charge processing fees for such requests. Total fees received and waived across government are set out in the following table. Break downs by Organisation appear at Appendix 2, tables 4 and 5.

Comparative table: Fees received and waived



FOI Correction applications

The scheme in the Act which allows people to apply to correct their personal information (Part 3, Division 3) is seldom utilised.

Anecdotally, it is understood that the correction provisions of the Act are not as well known by members of the public or within Organisations in comparison to the access provisions, and where a request may be made to an Organisation, this is likely to be managed in a manner that is not reported on.

The matters that make their way to a formal request under the Act are in most circumstances, complex, sensitive or otherwise difficult for Organisations to manage. The Act provides that Organisations may only correct a record where it is identified to be inaccurate, incomplete or out of date and personal information is not required to be corrected where it is identified to be historical only.

Where an Organisation determines a correction is required, they may elect to make the correction specified by an applicant or make a different correction of the Organisation's choosing. Where a different correction action is taken, the Applicant may request that a statement be associated with the record and an Organisation must take all reasonable steps to comply with this request.

In 2023/24, only two Organisations received applications to correct personal information. Of the four applications received in total, one application received the requested correction, one was not corrected, and two applicants withdrew their applications before a decision was made. None of these applications progressed to an internal review.

Timeliness measures for agencies

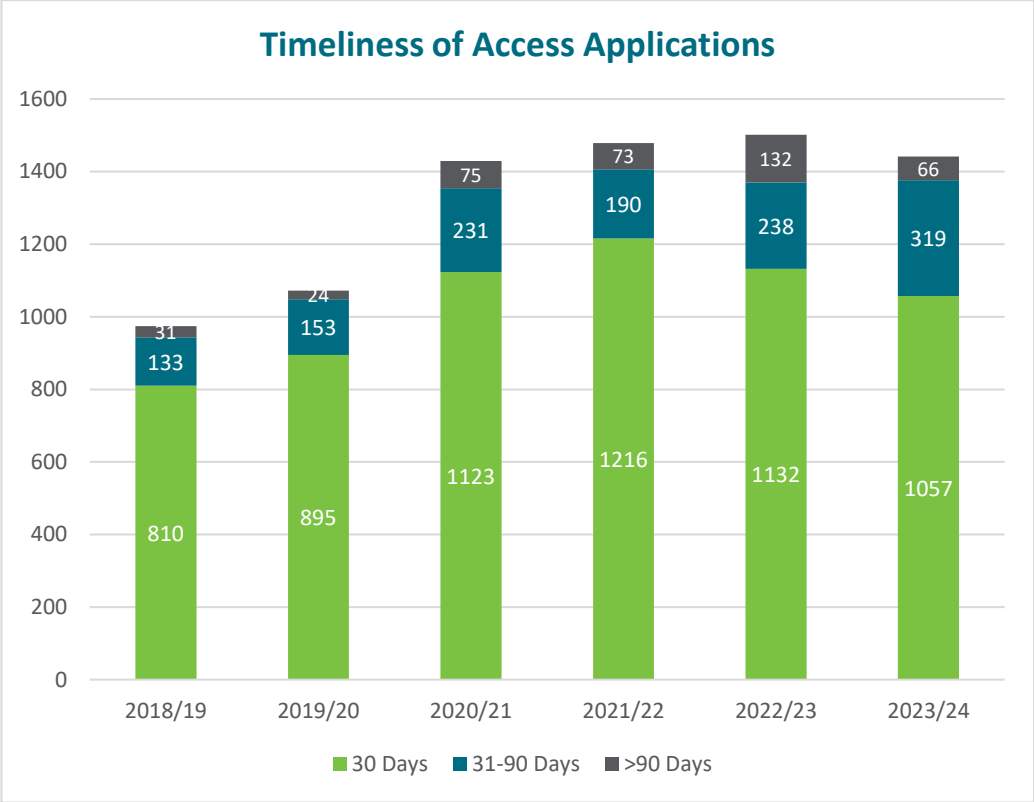
The Act provides legislative timeframes around notifications to applicants and Organisations are requested to provide statistical data to this Office on an annual basis. The data provided details the Organisations compliance with legislative requirements when finalising FOI applications within the first 30-day statutory timeframe or any valid extension period.

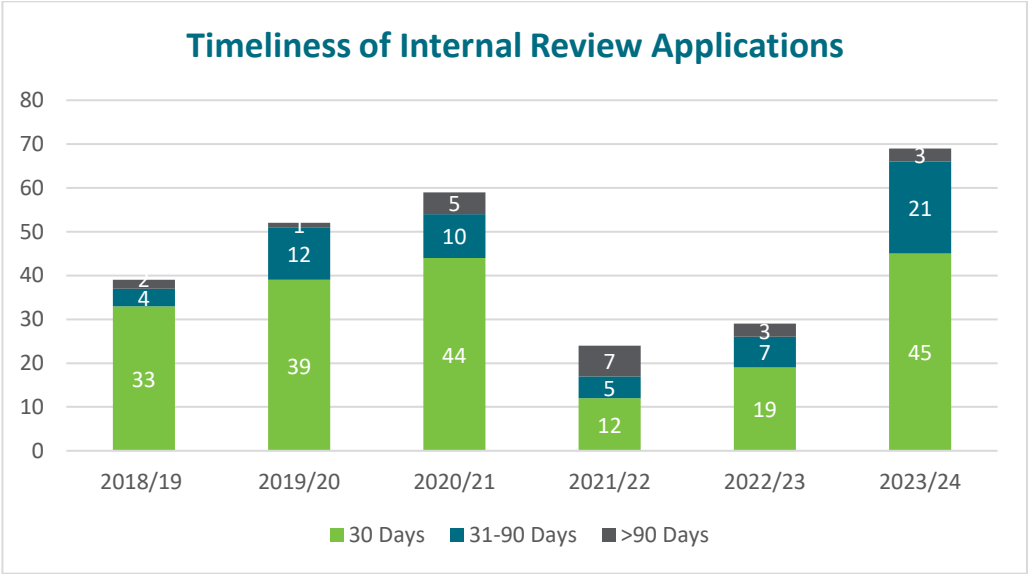
The Act provides for reasonable extension periods to provide decisions, where an application is related to a large amount of information or requires extensive searches, where consultation with third parties is required or where compliance with the 30-day period would otherwise unreasonably interfere with the operations of the Organisation.

Data on this measure provides a good indicator of how public bodies are managing an increasing workload and how the FOI scheme is working in terms of timeliness. This is of particular interest to this Office as the OIC has identified an increase in contact and enquiries from applicants regarding delays in finalising applications.

In 2023/24, the combined data of the Organisations showed that 72% of FOI applications were finalised within the first 30 days, with a total of 93% of applications being finalised within 90 days. It is notable that in the past 5 years, these proportions have largely remained static with only a slight decrease in time efficiencies since the 2021/22 reporting period (see graphs on next page for more).

In 2023/24, Organisations finalised 63% of internal review applications within the first 30 days, with 93% of all applications being finalised within 90 days.





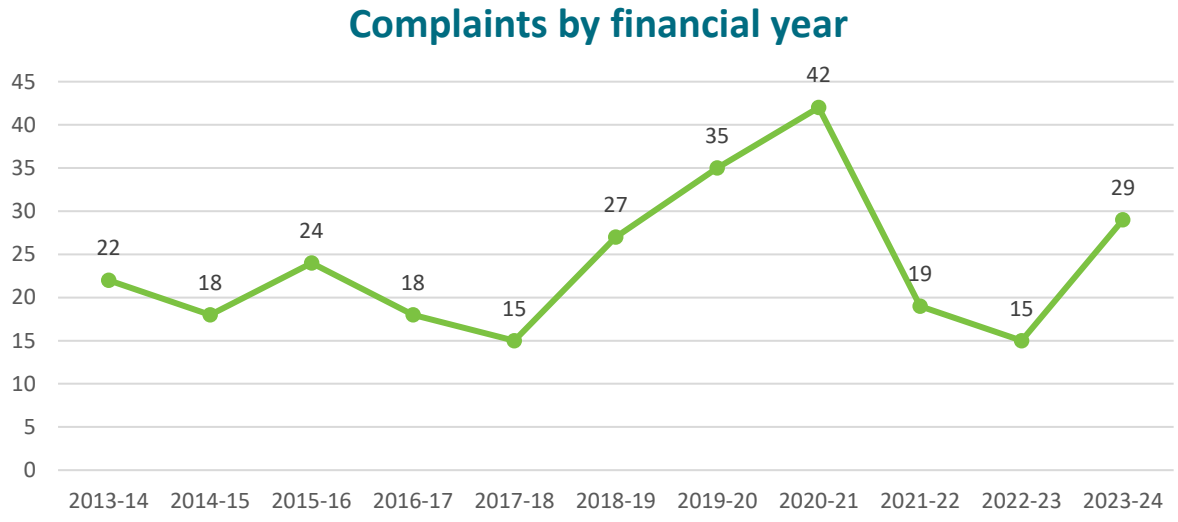
There appears to be no right on the part of an Organisation to extend the time for an internal review decision beyond 30 days. Failure to make a decision within that time could be taken as a deemed refusal providing a basis for a complaint to the OIC. However, there may well be good reasons for an Organisation taking longer in some cases, for example, a need to consult further with third parties. Organisations that consider a longer period is required for internal review are strongly encouraged to actively liaise with the applicant to explain the situation and seek agreement to allowing further time. We urge applicants to reasonably accommodate such approaches.

Exemption certificates

The Chief Minister may issue an exemption certificate certifying that government information identified in the certified is exempt for specific reasons set out in section 60 of the Act. No exemption certificates were issued by the Chief Minister during 2023/24.

FOI complaints to OIC

The number of FOI complaints received by the OIC increased this reporting period, from 15 in 2022/23 to 29 in 2023/24. This increase reflects the similar increase in access applications progressing to internal review. While it is too early to determine whether the increase in complaint numbers this reporting period will continue, we will monitor common themes and trends.



The table below lists the FOI complaints handled by our Office during this reporting period, (including 18 carried over from 2022/23).

Organisation	New Complaints	Carried Over	Finalised	Open at EOY
AAPA		1		1
AGD	2	3	4	1
BCGC	1		1	
CDU	2		1	1
CoD		1	1	
DCMC	1	1	1	1
DEPWS	1	2	2	1
DIPL	1			1
DoE	1	4	4	1
OCM	1	6	4	3
NTP	16		14	2
TFHC	3		2	1
TOTAL	**29**	**18**	**34**	**13**

Note: See Appendix 2 for the full names of abbreviated public sector organisations referred to in the table.

Over half of all complaints submitted to the OIC in 2023/24 related to decisions by NT Police. Of these complaints, 9 were submitted by one applicant and most related to questions of legal interpretation that may ultimately be considered by the NTCAT.

In 2023/24, the OIC finalised 34 complaints, an increase on the 2021/22[5] and 2022/23 [6]figures.

In appropriate circumstances, the OIC may refer a complaint back to the Organisation that made the decision and require it to conduct a further review of the decision. Of the complaints finalised by the OIC in 2023/24, 16 were referred back to the Organisation to re-review after investigation and consultation by the OIC. This was usually done on the basis of a preliminary view identifying deficiencies in the original decision or other reasons why a review by the Organisation was the preferred option. Historically, most matters referred back to the Organisation appear to have been resolved between the parties without the need for further consideration by the OIC.

During the period, one complaint progressed to the Northern Territory Civil and Administrative Tribunal (**NTCAT**).

Timeliness

During 2023/24, 16 complaints were finalised within 6 months of being received by the OIC and another 5 complaints were finalised within 12 months of receipt. Regrettably, 13 complaints finalised were over 12 months old. Generally, these older matters were particularly complex and issues in communicating with some complainants contributed to a delay in investigation. The limited resources available to the OIC to carry out its numerous functions was also a factor.

Complaint case studies

The power of negotiation

Where possible, the OIC will try to assist parties to reach a negotiated settlement. In this case, M was a passenger on an international flight to Australia which made an unscheduled landing at an NT Airport, due to a medical emergency. Upon landing, passengers were advised to stay on the plane for a period of approximately six hours, before being directed to move to and remain within a restricted zone in the airport terminal. M was not happy about the restrictions placed on him and wanted to understand why.

M submitted a FOI application to gain information about what had occurred on the flight, and why his liberty had been restricted. The Organisation provided M with partially redacted documents showing there had been a medical emergency on board, and heavily redacted documents about why his liberty had been restricted. In redacting this information, the Organisation relied on sections 56(1)(a) and 46(1)(a) of the Act, stating that the full release of the medical information would be an unreasonable interference with privacy, and the full release of information regarding the reasoning behind the restrictions on the complainant's liberty would prejudice the defence of the Commonwealth (or a state or Territory therein).

[5] 29 complaints closed in 2021/22
[6] 16 complaints closed in 2022/23

M subsequently raised a formal complaint with this Office seeking unredacted access to the information. After accepting the complaint and investigating, we reached the preliminary view that the Organisation was correct in limiting M's access to the medical information. However, we also considered the Organisation may have misapplied section 46(1)(a) because there was no basis to withhold access to information on the grounds that it would prejudice the security of the Commonwealth (or any state or territory therein).

We raised the potential for release of the information withheld under section 46(1)(a), while at the same time discussing with M the potential to withdraw their request for access to the redacted medical information. Ultimately the parties agreed and the matter was referred back to the Organisation to implement the agreed actions.

Unprofessional behaviour against the objects of the Act

This was an example of unprofessionalism that should not be seen in an Organisation. B submitted a request to an Organisation for CCTV footage relating to an alleged incident that he was involved in. The applicant sought 12 hours of footage which was refused by the Organisation, purportedly in accordance with section 25 of the Act and on the basis that it was not *manageable* or *practicable*. Ten days after receiving the refusal decision, B contacted the Organisation with a revised scope, reducing the footage request to a smaller and more reasonable period of time. The Organisation advised that the decision would be considered, and that B may expect a further response.

When the Organisation failed to contact B within a two-month period, B contacted the OIC to discuss the application and discuss his rights in this matter. The OIC spoke to the Organisation who agreed that a decision would be provided to B as a priority and in accordance with the Act. Seven months later, B again contacted the OIC for assistance as B had heard nothing from the Organisation.

When asked why B's request has not been processed, a representative of the Organisation blamed B for bothering them too often about the matter. The Organisation again committed to providing a response to B within a period of 30 days.

Two months later, B again contacted the OIC as he had not received a response from the Organisation. After further communication, the Organisation admitted to B that the CCTV footage no longer existed and had in fact been deleted after 30 days.

The outcome in this matter was most disappointing both for B and for the FOI process. When a request for CCTV footage is sought, the relevant recording should be immediately identified and preserved until the FOI process is finalised. The OIC will communicate our concerns to the Chief Executive Officer of the Organisation, so that the necessary steps can be taken to prevent a recurrence of the poor service experienced by this applicant and to prevent the unacceptable destruction of a government record that is the subject of a FOI application.

An unreasonable delay

The OIC received a complaint from D regarding the extensive amount of time it was taking for D's FOI application to be processed. D, an employee of the Organisation, had submitted a request for information relating to her employment and had been waiting 4 months for information. During this period, the Organisation had provided D with email correspondence on five different occasions, advising that more time was required to make a decision in accordance with section 26 of the Act.

After one such communication, D had objected to the reasons provided by the Organisation as to why the application was taking so long to finalise. D requested that the matter be escalated to a more senior member of staff. The Organisation did not respond or escalate the matter as requested by D.

The Act provides that a complaint cannot be submitted to the OIC about a FOI application unless the applicant has firstly requested the Organisation undertake an internal review of the decision. In this circumstance, while D had not formally requested that an internal review process be commenced, this Office formed a view that the objection that D raised in writing should have been considered further by the Organisation in the same manner as a request for a review.

The OIC approached the Organisation to better understand the reasons for delay in finalising the application. The Organisation agreed to prioritise the application and committed to providing a final decision within a period of 7 days. D agreed that this was acceptable, and the matter was considered resolved without progressing to formal acceptance and investigation.

D received the requested information shortly after.

NTCAT FOI proceedings

After a complaint has been finalised by the OIC, and where a matter cannot be resolved through the mediation process, an aggrieved party can apply to the Commissioner to refer a decision to the Northern Territory Civil and Administrative Tribunal (**NTCAT**) for hearing. In such cases, the OIC prepares a referral report to NTCAT and, in some cases, participates in the Tribunal proceedings.

In 2023/24, one FOI matter was referred to NTCAT and one matter was finalised by a NTCAT decision. While the referred matter is still before NTCAT, set out below is a summary of the Tribunal's decision in the finalised matter, which can also be found on the AUSTLII website.

SB v Northern Territory of Australia (published)

This matter concerns an application by SB seeking access to correspondence mentioning SB and/or their family member, and correspondence related to a formal administrative notice issued to them. 710 pages of information were found to be within the scope of the application, but the Organisation withheld some information on the basis that its disclosure would breach client legal privilege pursuant to s 49(d) of the Act and would unreasonably interfere with a person's privacy pursuant to s 56(1)(a) of the Act.

SB lodged an application with the Organisation for an internal review, which resulted in more information being released, however SB remained dissatisfied and lodged a complaint with the OIC. The OIC determined that there was sufficient prima facie evidence to substantiate SB's complaint and referred the matter to mediation.

An external mediator was appointed by OIC to deal with the matter and the mediation process extended from June 2022 to January 2023, resulting in further disclosures of information by the Organisation to SB but access to 23 pages of documents were refused under ss 49(d) and 56(1)(a) of the Act. The matter then progressed to an NTCAT hearing.

NTCAT deliberated on whether the exemptions were correctly applied to specific correspondence, particularly focusing on client legal privilege and privacy concerns. It considered the impact of any release on personal privacy and whether disclosure would serve the public interest under section 50 of the Act. Issues around the definition of “personal information” were discussed, for example disclosure of mobile phone numbers of public officers and a consideration of the personal impacts on individuals involved in a difficult matter.

Ultimately, NTCAT upheld the Organisation's exemptions for most contested information, finding that disclosure could unreasonably interfere with privacy and was not in the public interest. Despite the applicant's success in narrowing down the withheld information during the proceedings, NTCAT confirmed the Organisation’s decisions in large part, acknowledging the complexity and sensitivity of the issues involved.

This case is notable for its detailed analysis of the exemption under section 56(1)(a), particularly in regard to whether correspondence sent in an official capacity by a government employee qualifies as "personal information" under section 4A. It clarifies that even if such communication occurs in an official context, its release may still constitute an unreasonable interference with a public servant's privacy in certain situations. Therefore, a request for its release remains subject to the public interest test under section 50.

Privacy Protection

All Organisations are required to comply with the Information Privacy Principles (**IPPs**) found at Schedule 2 of the Act. The IPPs are the 'rules' that set out how Organisations must collect, use, disclose, secure and destroy the personal and sensitive information that they hold.

The role of the Information Commissioner is to act as a 'privacy watchdog' for the NT public sector.

In accordance with the Act, an Organisation interferes with a person's privacy if it contravenes an IPP, an approved code of practice or an authorisation made by the Information Commissioner. If an individual is concerned that an Organisation has breached their privacy, they must first provide the Organisation with an opportunity to resolve or rectify the matter. If the Organisation does not do so within a reasonable amount of time, the matter may be referred by the individual as a complaint to the OIC.

The OIC investigates and mediates privacy complaints in circumstances where the Organisation has been unable to resolve or rectify the matter. Our office tries to resolve complaints at an early stage where possible and this is often through a process of mediation.

Mediation allows parties to have open and frank conversations about an alleged breach of privacy and provides for an exchange of information in a protected setting. On occasion, this exchange of information may alter each party's perception of what occurred and/or help them understand the other's point of view. While some settlements are confidential, outcomes achieved at mediation can include payments of compensation, letters of apology and agreements by Organisations to undertake specific actions.

If matters don't resolve through the complaint processes within our Office, the individual can seek referral to the NTCAT for a decision as to whether or not a privacy breach has occurred and whether orders should be made to prevent ongoing action, rectify the breach or compensate the complainant.

The OIC allocates significant resources to providing advice and guidance to Organisations on privacy protection either in their day-to-day work or when they are implementing new initiatives. In addition, the OIC provides education and advice to the public on their privacy rights under the Act.

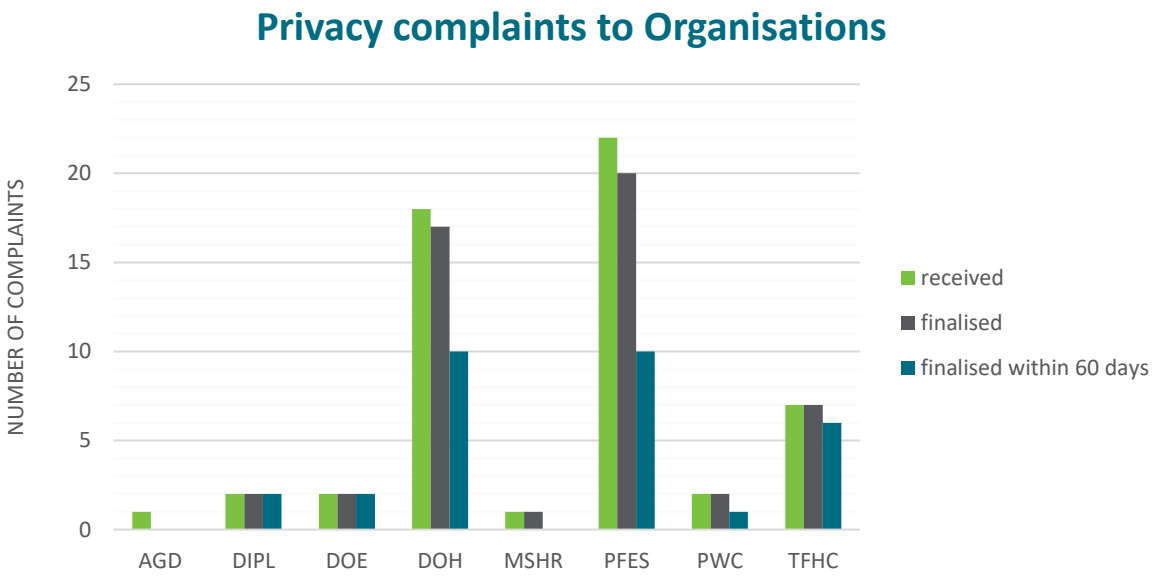
The public's understanding and expectations are shifting when it comes to privacy and data protection, and Organisations need to respond to those changes in expectations. A primary focus of the Office is about supporting Organisations in maintaining the integrity and security of the personal and sensitive information held and supporting members of the public in raising privacy concerns either directly with the Organisation or through this Office.

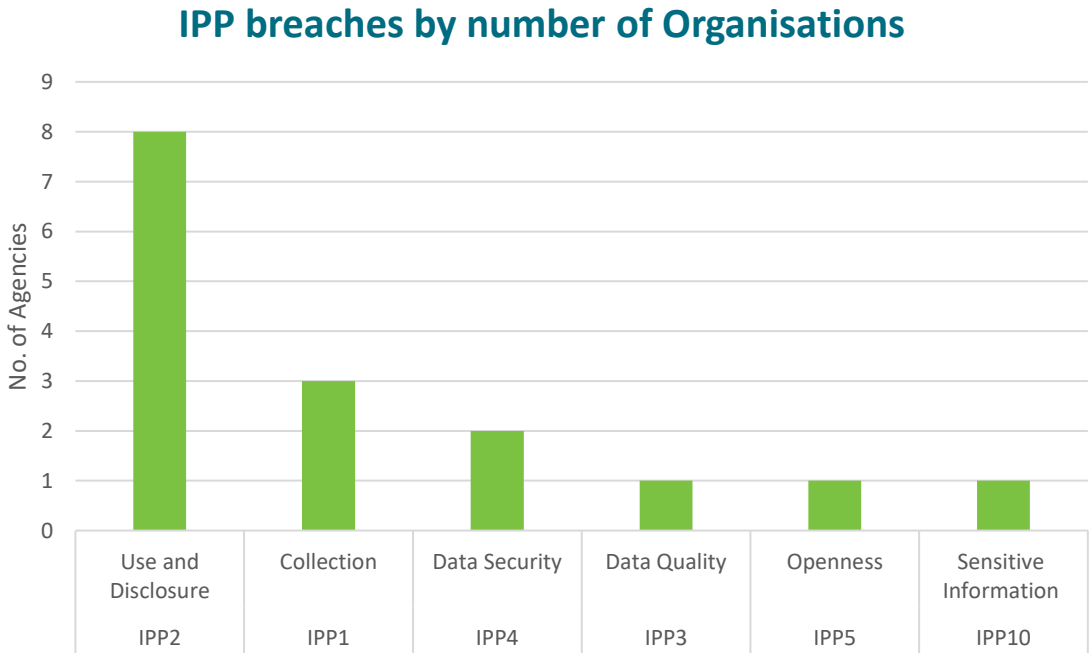
Privacy complaints to Organisations

In 2020/21, the OIC commenced annual reporting requests to Organisations for the purpose of gaining an appropriate insight into the management of privacy complaints. Historically, the OIC would only become aware of a breach of privacy when an individual escalated a complaint or where an Organisation voluntarily notified the OIC of the matter.

During 2023/24, Organisations reported the following:

- A total of 55 new privacy complaints were reported as received by 8 Organisations, with 6 complaints carried over from 2022/23.
- The privacy complaints alleged breaches of various IPPs, including collection of personal information (IPP 1), use and disclosure of personal information (IPP 2), data quality (IPP 3), data security (IPP 4), openness of information (IPP 5) and collection of sensitive information (IPP 10).
- Of the 61 privacy complaints managed by Organisations during 2023/24, 51 complaints were finalised in total, with 31 of these being resolved within 60 days. Ten complaints remained open at the end of the reporting period.
- Police and Health received the most privacy complaints of 22 and 18 respectively, although it should be noted that not all of these complaints were found to be substantiated.





Remedies

The focus on resolving a privacy complaint within an Organisation should be to ensure the incident is not indicative of a systemic or cultural issue and to consider what reasonable solution a complainant is seeking.

During 2023/24, the most commonly reported remedies agreed to by the parties in resolution of privacy complaints were:

- Organisations refraining from repeating or continuing to do an act;
- Organisations offering an apology for circumstances leading to a breach; and
- general changes to practices or systems to avoid or limit future breaches.

In addition to the above, some Organisations have introduced new policy and procedures around privacy breach identification and management as well as implementing internal privacy training and awareness.

Organisational reform

This year, the OIC recognises the efforts taken by some Organisations to implement reforms to improve operations around privacy and to introduce structure around the management of privacy and data breaches.

DIPL

The Department of Infrastructure, Planning and Logistics (**DIPL**) contacted the OIC this year, seeking advice and guidance in the drafting of stronger privacy policy and procedure. DIPL recognised that the distinct work functions of their Organisation had different levels of understanding around privacy requirements, and proactively sought to improve compliance with privacy laws.

DIPL sought to have in place a policy that would clearly outline the obligations on the Organisation regarding the collection, use, disclosure and protection of personal and sensitive information and that would be applicable to all staff and contractors.

This Office worked with DIPL to revise and strengthen their current policy, which provides clear direction to staff on what constitutes a breach and how one should be managed. At the time of this report, the DIPL Privacy Policy had been endorsed and disseminated throughout the Organisation.

The OIC commends the actions taken by DIPL in promoting the policy internally and continuing to ensure privacy protection is a priority of the Organisation.

DCDD

The Department of Corporate and Digital Development (DCDD) introduced a permanent privacy role to its Information Management Services work unit this year, with a primary objective that the position would assist the Agency in meeting its privacy obligations under the Act. The introduction of the position is welcomed noting privacy protection is a live issue in an agency that provides cross-government service delivery (e.g. corporate and digital services; information and communications technology (ICT); project management of development initiatives and advice on digital solutions).

DCDD has also prepared and implemented within its agency the Northern Territory Government Data Breach Policy (Personal Information) and related response plans and templates. The data breach policy details the obligations on Organisations regarding the management and notification of a data breach and the plan and template provides Organisations with advice on how to manage such an incident.

The OIC commends DCDD on the introduction of a privacy specific position and supports the introduction of strong policy and guidance to assist Organisations in the protection of personal information. This Office looks forward to supporting DCDD in ensuring the policy and supporting documents are appropriately promoted and disseminated to other agencies, as these, together with training and support, will greatly assist in helping to establish a cohesive privacy protection response across government generally.

Privacy complaints to OIC

Where a privacy complaint cannot be resolved by an Organisation, a complainant has a right to submit the complaint to the OIC. The OIC received two privacy complaints this year, which is a significant decrease from the number of complaints received in 2022/23. In addition to the two new privacy complaints, the OIC dealt with a further 5 complaints that were carried over from the 2022/23 reporting period.

Organisation complained about	New complaints	Carried over	Finalised	Open at EOY
AGD		1	1	
DIPL	1		1	
DoE		1	1	
DoH	1	2	3	
PWC		1	1	
TOTAL	**2**	**5**	**7**	**0**

Note: See Appendix 2 for the full names of abbreviated public sector Organisations referred to in the table.

Seven privacy complaints were finalised by the OIC in 2023/24. Of these complaints, two were not accepted as they either did not meet the requirements of section 104(2) of the Act or the complainant chose not to progress with the complaint.

A further four complaints were discontinued at the complainant's request or because of a lack of interest by the complainant in pursuing the matter. One complaint progressed to a *prima facie* decision under section 110 of the Act before being resolved at mediation.

There were no open privacy complaints at the end of the period.

Privacy breaches

There is no current legislative requirement on Organisations or public officers to advise the OIC when there has been a data (privacy) breach, however some Organisations will choose to proactively inform the OIC when an incident occurs, for the purpose of seeking advice and guidance on the appropriate management of a matter.

Organisations reported eight data breaches to our Office in 2023/24. The reported breaches were of varying levels of seriousness and occurred in both large and small Organisations. They included:

1-Disclosure of customer details to third party

A staff member accessed and disclosed personal information about Z to an external body. Although the Organisation assessed the breach as low risk, they contacted Z and advised of the steps being taken in response to the breach. This included the termination of a temporary employee and documented warnings to two other employees. Training was provided to all team members about the importance of not accessing information that is not required for work purposes. A review was also undertaken of induction training to ensure a greater focus was placed on the importance of privacy, confidentiality and the consequences of data/privacy breaches.

2- A technical error

A member of the public received 2 invoices in their envelope, with only one of the invoices relating to them. The second invoice containing name, address and non-sensitive information related to another person. An internal investigation disclosed that the incident occurred because of a technical error in the automatic enveloping of invoices. The Organisation advised that the error appeared to be an isolated incident and that there have been no further incidents. The customer whose privacy was breached was notified and the option of requesting electronic billing in the future was discussed with them.

3-Incorrect email recipient

A clerical error led to information about a person, including their address, being incorrectly emailed to another person. The recipient was contacted and confirmed that they had deleted the email. The person whose privacy was breached was also notified and the Organisation apologised for the error.

4-Access to generic mailbox wrongly provided to another

An employee of Organisation B was mistakenly granted access to a generic mailbox of Organisation A for less than a day. The mailbox included customer information and contact details. Once the breach was identified, the recipient's access was removed and an internal audit was undertaken to identify what went wrong. The audit confirmed that the breach was caused by human error. The recipient did not appear to be aware of their access to this mailbox and they confirmed to Organisation A that they had never tried to access it. A review of security breach processes was undertaken to ensure that if a data breach affecting more than one Organisation was identified, then the affected Organisation/s would be immediately notified. Work is also being undertaken to ensure that Organisation B only retains access to the information it needs for work purposes from Organisation A.

5-Human error meant access to website set to 'Public'

A user of an Organisation's Teams and Sharepoint sites notified management that they were able to view the personal information of others. An investigation found that the sites contained personally identifiable information about a significant number of users which was searchable by staff and other users who held an account with the

Organisation. Immediate action was undertaken to secure the identified sites by changing their status from 'Public' to 'Private'. An investigation disclosed that the misclassification of the sites as 'Public' was caused by human error. The investigation also disclosed that only one user appeared to have downloaded information about other users but that user confirmed that he had deleted the information and there was no evidence of exploitation to the contrary. All affected users were contacted, offered information and support and their queries were answered. No complaints have been received by our Office following this breach.

6-Incorrect email recipient

A staff member of the Organisation mistakenly sent a document with personal information to a contractor. The document included names and brief personal details of a number of persons who attended a meeting. The contractor promptly deleted the document and notified the Organisation. The risk to individuals was assessed as low due to the nature of the information shared and the contractor's understanding of privacy principles regarding work within the relevant Organisation.

7-Inappropriate disclosure to an outside organisation

A staff member mistakenly disclosed to an external contractor commercial information containing some names and contact details of various individuals working for external organisations. An internal investigation assessed the privacy risk as low as the personal information appeared to be related to each individual's work rather than their personal life. Advice was provided by OIC on ways to minimise future breaches.

8-Alleged improper disclosure under investigation

OIC were notified by an Organisation that a staff member had allegedly provided personal information about another to a third party. An internal investigation by the Organisation resulted in a report to the relevant authorities for further investigation and consideration of further action.

Mandatory data breach notification

When notified of a privacy breach by an Organisation, this Office provides advice about options for action and possible steps to minimise the risk of harm to the individuals affected. It is most important that affected individuals are made aware of any serious breach and that they are aware of their right to make a privacy complaint should they wish to do so. We also work with Organisations to minimise future risk and to improve their privacy protection and staff training.

There has rarely been a time when public concern about the protection of privacy has been more prominent. Recent cyber hacks have heightened public awareness and there is a real appetite on the part of people to know about how government and businesses are handling their data and when problems arise. With that in mind, it is important for Government to act to ensure a fair and consistent approach to handling data breaches and data breach reporting.

A number of Australian jurisdictions, including the Commonwealth[7], NSW and Queensland, have legislative mandatory data breach reporting requirements. These provide clear guidance for agencies on when breaches should be reported to the relevant oversight body and to affected people. They also provide for regular public reporting on notifications of serious breaches. They provide a standard which promotes organisational and public understanding of when reporting is required.

The OIC has worked with NT Government officers over time to advance development of a whole of government approach to data breach reporting but there is, as yet no effectively publicised system. As in previous years, I emphasise my strong view that the introduction of a robust mandatory data breach notification system, consistent with other Australian jurisdictions, would be a significant step in protecting the privacy of Territorians.

Privacy case studies

Staff misuse of government information

V contacted an Organisation to complain about an alleged access and disclosure of his personal information by a staff member of the Organisation. V claimed that they were advised of the breach by a witness, who became aware that the staff member had accessed V and his partners' personal information and disclosed it to a third party who was known to all parties. The third party then proceeded to use the information to their own advantage.

The Organisation undertook an investigation of the allegation and found that, while it was proven that the access to information had occurred, there was no evidence to support a further disclosure of the information as alleged. The investigation by the Organisation resulted in internal actions to resolve the matter and proactive notification to the OIC. The Organisation did not formally provide V with an outcome to the internal investigation.

V escalated a complaint to the OIC, stating that he was dissatisfied with the management of his complaint by the Organisation, and any subsequent outcomes. V stated that the actions taken by the third party were evidence of a disclosure of the information and advised that he sought financial compensation and to have disciplinary action taken against the staff member involved.

---

[7] The Commonwealth data breach scheme requires notification in the following circumstances:

An eligible data breach occurs when:

- *there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds*
- *this is likely to result in serious harm to one or more individuals, and*
- *the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action.*

The Office of the Australian Information Commissioner provides the following examples of serious harm:

- *identity theft, which can affect your finances and credit report*
- *financial loss through fraud*
- *a likely risk of physical harm, such as by an abusive ex-partner*
- *serious psychological harm*
- *serious harm to an individual's reputation.*

https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/what-is-a-notifiable-data-breach

This Office accepted the complaint and commenced investigation. After considering all available information, this Office formed a preliminary view that it was reasonable to determine that the inappropriate access of information had occurred, and a further disclosure of the information was likely to have occurred. The preliminary view was that actions of the Organisation contravened IPP 2 – Use and Disclosure and IPP 4 – Data Security.

This Office provided its preliminary views to the parties and sought to resolve the matter through a process of early mediation and informal resolution. While all parties initially agreed to an informal resolution to the matter, after consultation V advised this Office that he would prefer to put the matter behind him and chose to withdraw his complaint before mediation could commence.

Resolution through mediation

Q made a complaint to the OIC that an Organisation had interfered with his privacy by disclosing his personal information to a second Organisation. Q complained that the second Organisation had then further interfered with his privacy by disclosing the information to multiple individuals involved in a public event that took place in Darwin.

Q had previously raised the complaint directly with both Organisations, with the first Organisation finding that the use and disclosure of information was lawful and in accordance with section 70 of the Act and the IPPs. The second Organisation found that the use and disclosure of Q's personal information was supported by sections 69 (regarding limits on IPP compliance for matters before a Court or Tribunal) and 70 (regarding limits on IPP compliance for law enforcement agencies).

This Office decided to accept the complaint and commence an investigation of the matter. Our Office sought submissions from all parties to the complaint and considered the sections of the Act relied on by the Organisations to exempt them from the IPPs. Specifically, we considered Q's submission that the use and disclosure of his personal information to other individuals was not *necessary* for the functions of the Organisations.

Based on the available evidence, our Office made a *prima facie* decision that Q had an arguable case that the reliance on section 70 of the Act by each Organisation was not sustainable, and there had been an interference with his privacy. On finding that there was sufficient *prima facie* evidence to substantiate the matters complained of, the complaint was referred to formal mediation and was successfully resolved.

Other OIC operations

The past few years have seen a number of NTG Organisations upgrading their digital systems to better service Territorians and streamline organisational functions. The OIC has limited involvement in the technical aspects of the system upgrades but we continue to make ourselves available to advise agencies on ways to ensure that new technologies are respectful of each individual's right to privacy and compliant with the relevant IPPs in the Act.

Child protection data access agreements

Throughout the last two reporting periods, my Office has provided advice to Territory Families on a new technological solution to assist them in keeping vulnerable children safe (the **360VoC Solution**). The information sharing envisaged by this new digital solution will be supported by Data Access Agreements (**DAAs**) that approve the provision of information to Territory Families. The DAAs are authorised by changes to the *Care and Protection of Children Act 2007*. The amendments require the CEO of Territory Families to consult with my Office when entering into a DAA. An additional resource (a senior policy officer) was provided to the OIC to assist with this project.

In my 2021/2022 Annual Report, I provided an extract from correspondence to the CEO of Territory Families that remains relevant to this project:

> *There is no question that part of government's role in protecting a vulnerable child is to ensure that systems exist for the sensible sharing of information between agencies and others with a legitimate interest in the safety and welfare of the child. Throughout my time as Information Commissioner, I have strongly supported responsible information-sharing and encouraged proposals that provide for it. Similarly, the Coroner raised concerns about poor information sharing in a recent inquest and noted the earlier recommendations in the Little Children are Sacred report that addressed this issue. The Coroner's recommendations included that 'the Multi-Agency Community and Child Safety Framework be legislated so as to ensure mandatory cooperation, coordination and information sharing in a timely manner.' … I am supportive of the Coroner's comments and his recommendation to improve information sharing. …*
>
> *The concepts of responsible information-sharing concerning 'child safety and wellbeing' and the need for privacy protection are closely linked and are not mutually exclusive. If a child's safety is at risk, then a robust sharing of information is vital. … Wellbeing, however, is a very broad term that is defined in the Oxford dictionary as 'the state of being or doing well in life; happy, healthy, or prosperous condition'. … Wellbeing includes an individual's right to privacy unless there is good reason otherwise. …*
>
> *There is … danger in legislation that oversteps the mark in terms of ostensible legal authority to collect, leading to families, non-government organisations and indeed professionals within government agencies, failing to record information or recording minimal information in case it is sought under the legislation. This could lead to drying up of available information which would be in no-ones interests.*
>
> *As I have stated on numerous previous occasions, it is important that stakeholders be engaged and supportive of the undoubtedly valuable policy aims of the legislation, if information-sharing is to be truly effective.*

From the outset, the position of my Office has been to accept the underlying importance of reasonable information sharing in this context, while robustly testing whether the scope and mechanisms for such sharing exceeds what is reasonably required to meet the policy aims of Government.

The technological solution will involve automated provision to Territory Families of a range of specified personal information held by a range of agencies, relating to children who have involvement with Territory Families, including those in their lives who are considered to be a 'close connection.'

This is a very broad information sharing scheme, involving information about a substantial number of Territory families, held by bodies as diverse as NT Police, Health, Education, Housing, Courts and Correctional Services. The intention behind obtaining so much information is to provide a 360 degree view of the life of a child for use by Territory Families in making decisions about their care and protection. The information will be available to Territory Families' authorised users through the CARE System, the operational child protection system.

Any cross-agency information-sharing agreement takes collaboration and a clear, common goal to ensure the best outcome for stakeholders. Throughout the past 2 years, relevant agencies have spent considerable time and effort working with Territory Families, the Department of Corporate and Digital Development (who are designing and building the technological solution) and my Office to reach agreement on what personal information should be available to Territory Families, who will have access to it and how it will be protected.

During 2023 and 2024, considerable public and stakeholder consultation was undertaken by the lead agency to inform and receive feedback. As part of the consultation process, a website was published providing stakeholders with access to information about the scheme[8].

During the reporting period, I made four related Grants of Authorisation under section 81 of the Act to assist the relevant Organisations in the technical build of the 360VoC Solution by allowing the development team to access limited personal information from each participating Organisation to facilitate matching information from disparate IT systems. The access approved by the grants was limited to information judged to be required to test the software and advance the technical build. Safeguards were put in place to ensure that the personal information accessed during this development stage remains safe and secure.

At the time of preparing this report, work is still continuing on the 360VoC Solution. Work also continues on developing the governance, guidance, training and support required to ensure that the information sharing aims of this significant project are achieved in a safe and supportive manner.

Domestic & family violence information sharing review

Amendments to the *Domestic and Family Violence Act 2007* (the **DFV Act**) aimed at improving information sharing came into force on 30 August 2019. They were aimed at assisting government agencies and non-government organisations involved in supporting victims and families to responsibly share information to keep victims safe.

[8] https://tfhc.nt.gov.au/children-and-families/changes-to-information-sharing

The information sharing amendments are contained in Chapter 5A of the DFV Act. Section 124U of the DFV Act required the Information Commissioner to review the first 2 years of operation of this Chapter, and later to review the 3rd to 5th years. Each review must include consultation with the Minister and with information sharing entities (**ISE**s). It must also consider any adverse effects of these reforms. The Act provides that the Information Commissioner's report to the Minister for tabling may include any recommendations on any matter addressed in the review.

The first review Report, titled *A Matter of Trust: First Review of Chapter 5A, Domestic and Family Violence Act* (the **Report**) was provided to the relevant Minister in December 2023 and tabled in Parliament on 15 March 2024[9]. The Report followed a considerable period of research, consultation and consideration of formal submissions and informal feedback received from stakeholders.

One of the themes that re-occurred during the consultation was the importance of stakeholders gaining and maintaining a trust in the information sharing scheme, including that personal information about a DV situation would be used for proper purposes. Hence the title: *A Matter of Trust.* At the time of finalisation of the Report, it was difficult to conclude with confidence that all stakeholders had gained trust in and were utilising the new scheme as envisaged.

In the Report, I commented on the challenges of introducing and educating stakeholders about a new information sharing scheme. I said:

6. *The domestic and family environment can present an incredibly complex set of constantly evolving challenges. Individuals may vary in their capacity, situational ability and willingness to make decisions that impact on their welfare (including decisions about information sharing) but the right to self-determination should be the starting point. Any departure that takes decision-making out of the hands of the individual should be carefully justified and closely monitored.*

7. *Departures for sound public interest reasons can be justified. A number of general departures already exist, for example, in Information Privacy Principle 2 in the Information Act. However, departures should only be maintained to the limited extent necessary and for so long as they are found to be effective.*

8. *This review therefore endeavoured to investigate the actual extent of information sharing under Chapter 5A, any concerns raised by information sharing and any identified hurdles or barriers to the effectiveness of the scheme. The timeframe for the initial review, limits on capacity within the Office of the Information Commissioner (**OIC**) and external factors have all meant this first review was targeted and strategic in both its consultation process and in its ultimate recommendations on what is required to strengthen the scheme. In conducting the review however, it became clear that Chapter 5A must be recognised as but one element among a variety of information sharing and co-operation mechanisms designed to facilitate compatible and effective community approaches to DFV. The review has therefore considered its operation within that broader context.*

[9]View the published report at https://infocomm.nt.gov.au/__data/assets/pdf_file/0008/1357244/DVIS-Report-Final-18Dec23-Incl-2-Annexures.pdf

A matter of trust

9. *Given the intrusion Chapter 5A permits into the lives of individuals, it is essential that they are provided with sufficient information to develop trust that it is implemented for their benefit. While there is an important role in this regard for Territory Families, as the lead agency responsible for Chapter 5A, an essential supplement can be provided by domestic violence service providers, particularly NGOs, who are often in the best position to explain and provide assurance to individuals whose information is being used and disclosed.*

10. *There are a large number of government agencies and NGOs working towards the same goal in the DFV sphere. While all have an underlying aim to work against DFV, their approaches and mechanisms for doing so may vary greatly. They include NGOs and health/social welfare agencies with a focus on providing care and service to individuals — with officers who have professional obligations to maintain confidentiality. There are law enforcement agencies who are often first responders to DFV situations but also have obligations to make and seek domestic violence orders and enforce the criminal law. And there are agencies responsible for making child protection orders and undertaking public housing or other government functions.*

11. *There are rarely easy answers as to the best course of action in DFV matters. The impacts of disclosure or a particular course of action are not always positive. The differing perspectives of these organisations and officers give rise to many differing views about the best ways to achieve positive outcomes in a DFV context. They can equally lead to diverging and, at times, diametrically opposed views on the best approaches to dealing with DFV and the sharing of information. This variance in preferred approaches can, and often does, lead to scepticism or, at least, wariness about how shared information will be used. Effective information sharing and co-ordination must be built on a high level of trust.*

12. *Parliament has provided a clear statement of intent by passing Chapter 5A that responsible information sharing is to be encouraged. Sending this message is no doubt one objective of the legislation and it may, without any formal reference to the scheme, be translating into greater effective information sharing. There is certainly a substantial amount of DFV information sharing between a wide range of government agencies and NGOs in a variety of forums.*

13. *However, it is difficult to say, on the limited evidence available, that the specific mechanism in Chapter 5A is being regularly utilised. There is a lack of records showing reliance on Chapter 5A and anecdotal evidence does not support an acknowledged, widespread reliance on its provisions. By the same token, nor is there any indication of privacy complaints or breaches being identified as associated with Chapter 5A information sharing.*

The clear need for stakeholders across the NT to gain greater knowledge of, and trust in, the Chapter 5A process informed a number of my recommendations, principally related to additional training, support and consultation about the scheme[10]. Other recommendations were geared towards supporting information sharing generally and to ensuring that the impacts of Chapter 5A reforms are properly evaluated.

[10] For Recommendations, see pages 21-25 of the published Report.

Although it is pleasing to note that 19 non-government organisations have now applied for and been approved as 'Information Sharing Entities"[11] I am not confident that sufficient resources and priority have been allocated to improve and support stakeholders to ensure the policy objectives of the scheme bear fruit.

It is early days however, and perhaps a better time to see progress (if any) will be during a second legislated review of the 3rd to 5th years of the operation of Chapter 5A scheme **(**, which is scheduled to commence in 2025. Once again, it is anticipated that the second review will require considerable research, consultation and feedback from stakeholders – including on the implementation of my recommendations.

The resource implications of my small Office undertaking a second review led to my inclusion of Recommendation 10 in the Report stating:

> *That the five-year statutory review be sufficiently funded to enable the Information Commissioner to engage appropriate experts and provide a more in-depth analysis and review of the impact and outcomes of the Chapter 5A reforms. For example, consultation with victims and questionnaires and surveys targeted at different stakeholder interests require specific expertise in communication, design and interpretation, particularly if the voices of victims, including Aboriginal victims, are to be considered.*

Recommendation 10 had earlier been provided to the lead agency for its comment but was not supported. Consequently, at page 24 of my Report, I stated:

> *Draft Recommendation 11 (now final Recommendation 10) notes the importance of providing sufficient funding for the 5-year review. The [NTG] response suggested that review funding is a matter for the Information Commissioner and their funding body. With respect, this is not a statutory review of the Information Act but a review required under the DFV Act. Monitoring and review is an important part of any initiative but Chapter 5A of the DFV Act falls squarely within the responsibility of Territory Families and financial responsibility for the conduct of such a review rests squarely with it.*
>
> *Reviews such as this are incredibly resource intensive and are difficult to complete in a fulsome or timely manner, if at all, for a small independent oversight body such as the OIC. It is not a matter for my Office to seek to obtain funding for a review of this nature relating entirely to an area within the responsibility of Territory Families. The unfunded resources required to conduct this first review have already substantially diverted our time and efforts from other statutory obligations. An effective 5 year review will require considerably more work, likely including engagement of expert professional assistance. As noted previously, if information sharing (and review to establish whether or not it is working) is considered worthwhile, it needs to be adequately funded and that is a matter for Territory Families to resolve.*

My Office should not have to bear the burden of finding resources to undertake the second review. Noting the importance Territory leaders place on improving outcomes for victims of domestic violence and their families, a meaningful report based on considerable consultation should be the aim. The need for reasonable resources for the second review should be acknowledged and appropriate resources allocated to the OIC to do the work.

---

[11] Published and current as at July 2024 at https://tfhc.nt.gov.au/__data/assets/pdf_file/0011/719336/information-sharing-entities.PDF

General enquiries

The OIC receives enquiries from Organisations, non-government organisations and members of the public about the FOI scheme and privacy rights and obligations. While individuals may attend the Office in person, most enquiries are received via telephone and email.

Common questions raised by members of the public relate to:

- guidance in submitting an application to an Organisation;
- explanation on the jurisdiction of the Act and referral to other oversight bodies where applicable;
- how to submit a complaint to, or access information held by, a non-government organisation or private company;
- questions on the management of FOI applications by Organisations, including explanation of decisions being provided to applicants.

Enquiries from Organisations are typically more complex and may involve such matters as:

- seeking the Commissioner's position on a specific wording in the Act;
- explanation of legislative provisions of the Act, including refusals of information and extensions of time to respond;
- seeking guidance and advice on how to manage a privacy / data breach;
- seeking the views of the Commissioner on proposed policy and procedure surrounding information sharing and privacy.

During 2023/24, the OIC recorded 270 general enquiries, in addition to formal complaints and applications, with:

- 155 enquiries relating to FOI matters;
- 97 enquiries relating to privacy matters; and
- 18 enquiries relating to other matters such as policy advice.

Advice and comment on policy and legislative changes

One of the key roles of the Office is to provide expert advice around all aspects of FOI and privacy matters at an early stage, to assist with the implementation of new initiatives in a way that promotes transparency and accountability, and reasonable information sharing, while treating personal information with appropriate care and in accordance with legislative requirements.

While staff in the Office are not able to provide legal advice, they regularly provide professional guidance and support to Organisations during the development and review of practices, policy and legislation. Advice is largely provided on an 'on-request' basis, so the hours recorded fluctuate depending on the types of initiatives being developed by Organisations and the extent to which the Office is approached for assistance.

During 2023/24, the OIC recorded 1,700 hours of advice provided to Organisations and other stakeholders on matters relevant to the Act, mainly on privacy and information sharing issues.

Topics covered included:

- Advice on appropriate information sharing between government agencies and sharing with entities outside the NT Government;
- Advice on how to best manage a privacy and/or data breach;
- Comment on the implementation of new policy and procedure around privacy and data breaches;
- Advice on whether the access, use and disclosure of personal information held with Organisations to the Commonwealth government complied with relevant privacy laws;
- Comment on proposed legislation impacting on the rights of individuals from a privacy perspective;
- Advice on access to CCTV footage held by Organisations;
- Advice and comment on recommended changes to the Act.

Awareness, education and training

During 2023/24, the Office continued to ensure delivery of regular engagement activities to Organisations and the public. Where resourcing made it impracticable for the OIC to attend an outreach activity in person, staff from the Ombudsman's Office assisted with promotion and raising awareness on behalf of the OIC.

Community engagement

Katherine outreach

A visit to Katherine saw material supplied to various stakeholders promoting the OIC's role. This trip provided an opportunity to meet members of the public, hold a pop-up stall at the Katherine Public Library and attend the Katherine Council on the Ageing (**COTA**) Seniors Expo.

Darwin outreach

An officer from the OIC attended the COTA Seniors Event 'Tuesday Talkies' held at Casuarina Square to raise awareness and answer any questions from the public about the work of the office. Many people approached the stall for more information about what we do and how to reach out.

Visits to various MLA offices

Brochures for the OIC were distributed to MLA offices across the NT during joint visits with the Ombudsman's Office to Alice Springs, Darwin, Palmerston, and Katherine.

Training for NTG agencies

In February and March 2024, the OIC assisted with the facilitation of FOI Training conducted by an external FOI expert. The training was attended in person by approximately 40 participants from across various NT government agencies.

The first day of the Information Officer training session provided an overview of the Act, including information and records management requirements, FOI processes, exemption provisions and charges.

The second day of the training focused on decision-making and applying the exemption provisions of the Act.

There continues to be an ongoing demand for the provision of this training.

Privacy Awareness Week

Privacy Awareness Week (**PAW**) is held annually each May, highlighting the importance of protecting personal information for the public and officers from government agencies.

The OIC promoted PAW and it's theme 'Power up your privacy' on its website, highlighting the relationship between privacy and technology and improving transparency, accountability and security.

Useful links to events being held for PAW were published, as well as resources and tips for individuals, government and businesses. To reach a wider audience, information was also circulated to privacy contacts within the government promoting these resources.

During PAW, DCDD offered internal training sessions to all staff, focusing on privacy awareness within government. The Commissioner and other staff attended multiple sessions and conducted presentations relevant to this year's theme.

International Access to Information Day

Annually on 28 September, the OIC celebrates International Access to Information Day, also known as Right to Know Day. The theme for 2023 was 'Digital inclusion: Connecting people to information'. A joint statement from Information Commissioners across the country was published on our website and a link to more information about the day was provided to stakeholders.

National and international cooperation

Tech in Gov conference in Canberra

In August 2023, the Deputy Commissioner travelled to Canberra as a guest speaker and panel member at the Tech in Gov conference - a leading event for government, IT and executive professionals involved in Digital Transformation, Cyber Security, AI and more.

The topic was, 'Navigating emerging technologies-wise words from a privacy perspective' and the panel discussion was focused on overcoming barriers to cloud adoption, including the need for privacy protection to be included in the early design stage.

Association of Information Access Commissioners (AIAC)

The Information Commissioner, together with other commissioners and ombudsmen in Australia and New Zealand, is a member of the AIAC. All members have a complaint and review jurisdiction over access to information legislation. Meetings are held twice a year to collaborate and discuss common issues and share knowledge and resources between jurisdictions.

Privacy Authorities of Australia (PAA)

The Information Commissioner is a member of a group comprised of commissioners and ombudsmen with jurisdiction over privacy laws in Australia. Meetings are held twice a year.

Asia Pacific Privacy Authorities (APPA)

The OIC is a member of APPA, a forum for privacy authorities in the Asia Pacific region. It gives privacy authorities in the region an opportunity to form partnerships, discuss best practices and share information on emerging technology, trends and changes to privacy regulation. An APPA forum is held annually as an opportunity for delegates to meet and discuss current and emerging issues in privacy and data protection.

Appendix 1 - OIC Financials

Detailed financial information regarding OIC operations now appears in the Ombudsman's Annual Report (in particular see the '*Comprehensive operating statement by output group*' at note 3 to the Financial Statements). A summary is set out below.

Figures have been rounded to the nearest thousand dollars, with amounts of $500 or less being rounded down to zero. Figures may not equate due to rounding.

OFFICE OF THE INFORMATION COMMISSIONER EXPENSES

For the year ended 30 June 2024

	2023-24
EXPENSES	**$000**
Employee expenses	429
Administrative expenses	37
Purchases of goods and services	*34*
Accommodation	2
Communications	2
Information Technology Charges	12
Insurance Premiums	1
Legal Expenses	5
Marketing & Promotion	-
Memberships and Subscriptions	1
Motor Vehicle Expenses	5
Official Duty Fares	2
Training and Study Expenses	3
Travelling Allowance	1
Property management	*3*
TOTAL EXPENSES	**466**

NOTE: Some categories of expenses are incurred by the Business Services Unit on behalf of all Ombudsman's Office work units. These include records storage, consumables/general expenses and stationery. They do not appear above.

Appendix 2 - Statistics by Organisation

The following public sector organisations received or handled FOI applications during 2023/24. The abbreviations reflect titles and responsibilities at 30 June 2024.

Abbreviations for public sector organisations

AAPA	Aboriginal Areas Protection Authority
AGD	Dept. of the Attorney-General and Justice
BGCG	Belyuen Community Government Council
BRC	Barkly Regional Council
CDU	Charles Darwin University
CMC	Dept. of the Chief Minister and Cabinet
CoD	City of Darwin
CoP	City of Palmerston
DCDD	Dept. of Corporate and Digital Development
DEPWS	Dept. of Environment, Parks and Water Security
DIPL	Dept. of Infrastructure, Planning and Logistics
DITT	Dept. of Industry, Tourism and Trade
DoE	Dept. of Education
DoH	Dept. of Health
DTF	Dept. of Treasury & Finance
ICAC	Independent Commissioner Against Corruption
KTC	Katherine Town Council
LRC	Litchfield Regional Council
NTEC	Northern Territory Electoral Commission
NTLAC	Northern Territory Legal Aid Commission
NTP[12]	Police Force
OCM	Office of the Chief Minister
OCPE	Office of the Commissioner for Public Employment
OO	Ombudsman's Office
PWC	Power and Water Corporation
TFHC	Dept. of Territory Families, Housing and Communities
TIO	Territory Insurance Office
WARC	West Arnhem Regional Council

[12] NT Police separated from the Fire and Rescue and Emergency Services in March 2024. The Police figures referenced in this report may contain approaches relevant to those functions.

TABLE 1 – Access applications and outcomes 2023/24

Details as advised by Organisations.

Org	Total Lodged	Full release	Part release	All exempt	Finalised other basis#	Total Finalised*
AAPA	1	0	1	0	0	**1**
AGD	266	25	100	11	103	**239**
BCGC	1	1	0	0	0	**1**
BRC	2	0	0	2	0	**2**
CDU	12	8	1	0	2	**11**
CMC	26	3	8	2	11	**24**
CoD	9	1	8	0	0	**9**
CoP	4	0	1	0	3	**4**
DCDD	13	3	5	0	11	**19**
DEPWS	45	6	10	2	20	**38**
DIPL	63	9	21	3	29	**62**
DITT	24	3	9	2	12	**26**
DoE	42	5	19	1	22	**47**
DoH	545	265	85	0	193	**543**
DTF	1	1	0	0	0	**1**
ICAC	6	0	2	4	0	**6**
KTC	3	3	0	0	0	**3**
LRC	1	0	0	0	1	**1**
NTEC	1	0	0	0	0	**0**
NTLAC	1	0	0	0	1	**1**
NTP	341	28	140	79	108	**355**
OCM	11	0	2	1	12	**15**
OCPE	1	0	1	0	0	**1**
OO	1	0	0	0	1	**1**
PWC	1	0	0	0	1	**1**
TFHC	372	35	213	12	127	**387**
TIO	4	4	0	0	0	**4**
WARC	1	0	1	0	0	**1**
Total	**1,798**	**400**	**627**	**119**	**657**	**1,803**

Notes:

For more detail on applications with other outcomes, see Table 1A.

* Outcomes may include matters carried over from the previous period.

TABLE 1A – Access applications finalised on another basis 2023/24

Details as advised by Organisations.

Org	Withdr	Transf	s18	s27	Fees	Excl	s25	Other	Total
AGD	22	11	34	28	0	1	6	1	**103**
CDU	1	0	0	1	0	0	0	0	**2**
CMC	2	1	1	5	2	0	0	0	**11**
CoP	0	0	0	0	0	3	0	0	**3**
DCDD	2	4	0	1	1	0	3	0	**11**
DEPWS	10	1	2	3	2	1	1	0	**20**
DIPL	11	1	9	2	0	1	3	2	**29**
DITT	3	0	2	6	1	0	0	0	**12**
DoE	6	1	3	12	0	0	0	0	**22**
DoH	21	1	129	28	14	0	0	0	**193**
LRC	0	0	0	0	1	0	0	0	**1**
NTLAC	1	0	0	0	0	0	0	0	**1**
NTP	40	4	13	17	14	15	1	4	**108**
OCM	0	5	0	1	5	1	0	0	**12**
OO	1	0	0	0	0	0	0	0	**1**
PWC	0	0	0	0	0	0	0	1	**1**
TFHC	9	0	18	97	1	0	1	1	**127**
TOTAL	**129**	**29**	**211**	**201**	**41**	**22**	**15**	**9**	**657**

Notes:

Withdr	Withdrawn
Transf	Transferred
s18	Invalid application
s27	Information does not exist, could not be identified or located
Fees	Non-payment of fee or deposit
Excl	Excluded from application of the Act or not covered by Act
s25	Unreasonable interference with operations
Other	Any other reason

TABLE 2 – Information correction applications and outcomes 2023/24

Details as advised by Organisations.

	Lodged	As Requested	Other Form	No Change	Withdr	Finalised
AGD	1	0	0	0	1	**1**
NTP	3	1	0	1	1	3
TOTAL	**4**	**1**	**0**	**1**	**2**	**4**

TABLE 3 – Internal Review applications and outcomes 2023/24

Details as advised by Organisations.

	Lodged	s103(2)	Confirmed	Varied/ Revoked	Withdr	s39A	Finalised
AGD	20	0	10	6	2	0	**18**
BCGC	1	0	0	0	0	1	**1**
CDU	2	1	0	1	0	0	**1**
CMC	4	0	3	0	1	0	**4**
CoD	2	0	1	1	0	0	**2**
DEPWS	5	0	3	1	0	0	**4**
DIPL	4	0	1	2	0	0	**3**
DITT	0	1	0	1	0	0	**1**
DoE	3	0	0	3	0	0	**3**
DoH	2	0	0	1	1	0	**2**
NTP	30	8	12	8	2	8	**30**
OCM	2	0	1	0	0	0	**1**
TFHC	7	0	6	1	0	0	**7**
TOTAL	**82**	**10**	**37**	**25**	**6**	**9**	**77**

Note: In addition, a small number of applications were carried over from 2022/23.

TABLE 4 – Application Fees 2023/24

Details as advised by Organisations.

Organisation	Fees Received	Reduced/ Waived	Reduction
AAPA	30	0	0
AGD	1140	5	150
BRC	30	0	0
CDU	60	0	0
CMC	660	1	30
CoD	240	1	30
CoP	90	1	30
DCDD	150	0	0
DEPWS	1260	1	30
DIPL	1290	2	60
DITT	600	0	0
DoE	240	1	30
DoH	3390	22	660
DTF	30	0	0
ICAC	60	4	120
KTC	90	0	0
LRC	30	0	0
NTEC	0	1	30
NTP	4770	5	150
TFHC	240	10	300
TIO	0	4	120
TOTAL	**$14,400**	**58**	**$1,740**

TABLE 5 – Processing Fees 2023/24

Details as advised by Organisations.

Organisation	Fees Received	Reduced/ Waived	Reduction
AAPA	30.00	0	0
AGD	6939.69	26	925.22
BCGC	0	0	0
CDU	0	0	0
CMC	1874.50	5	475.00
DCDD	150.00	0	0
DEPWS	3788.36	3	106.25
DIPL	6579.07	0	0
DITT	3595.92	3	326.94
DoE	1288.98	5	922.30
DoH	6460.34	20	2175.50
DTF	30.00	0	0
NTP	5809.00	3	125.00
TFHC	0	9	4851.25
TOTAL	**$36,545.86**	**74**	**$9,907.46**

Office of the
Information Commissioner

GPO Box 1344 Darwin NT 0801

Freecall 1800 005 610

infocomm@nt.gov.au

http://www.infocomm.nt.gov.au

NT House, 22 Mitchell Street

Darwin NT 0800